Построение отказоустойчивых систем автоматизации технологических объектов

П.Г. Нестеренко, К.Е. Пачуев, И.Н. Бухарин (ЗАО "ЭлеСи")

Рассматриваются вопросы построения автоматизированных систем управления с заданными параметрами надежности и избыточности. Приводятся примеры построения подобных систем на базе контроллера ЗАО "ЭлеСи".

В последнее время наблюдается оживление рынка систем промышленной автоматизации как в России, так и за рубежом. Основные производственные фонды российских предприятий требуют серьезной модернизации, что стимулирует развитие рынка АСУТП и встроенных систем. Как правило, заказчика систем управления интересуют системы повышенной надежности или, другими словами, отказоустойчивые системы.

Отказоустойчивое решение должно гарантировать исполнение функционала системы даже при наличии неисправностей [1]. Это означает не только применение высоконадежных элементов, а скорее проектирование системы таким образом, чтобы отдельные неисправности не влияли на ее работу в целом. В простейшем случае отказоустойчивая технология основывается на некоторой избыточности. Если какая-то часть, аппаратная либо программная, не работает, то ее заменяет другой компонент. Можно обозначить различные типы избыточности:

• физическая возникает за счет резервирования некоторых элементов, в том числе под физической избыточностью можно понимать избыточность аппаратной части для обеспечения диагностики состояния оборудования;

• информационная используется, например, в коммуникационных протоколах в виде служебной информации, добавляемой к пакету, чтобы обеспечить восстановление искаженных сообщений [2].

Таким образом, основной принцип повышения надежности – применение схем резервирования элементов системы. Резервирование – способ обеспечения надежности и увеличения наработки на отказ объекта за счет использования дополнительных средств и/или возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функции. Цель резервирования – обеспечить безотказность объекта в целом в момент отказа одного или нескольких резервируемых элементов [3]. При решении проблемы повышения надежности "в лоб" с помощью применения схем резервирования всех элементов системы, то есть общего резервирования, возникают два совершенно противоречивых требования. Сделать как можно более надежную систему, с одной стороны, а с другой – минимизировать затраты на создание системы. По опыту проектирования систем можно смело утверждать, что системы с полным резервированием стоят на порядок (иногда на несколько порядков) больше, чем системы без резервирования. Один из путей решения данного противоречия – резервирование только критичных к отказам элементов или элементов системы с меньшей надежностью, то есть раздельное резервирование.

Перед разработчиками была поставлена задача создания решения, позволяющего формировать системы управления [4] разной степени отказоустойчивости [5]. Для решения данной проблемы на основании опыта создания АСУТП были выделены основные факторы, обеспечивающие повышенную отказоустойчивость системы, построенной на базе ПЛК. Были выделены следующие основные факторы:

1. Резервирование системы электропитания, как наиболее критичного и ненадежного элемента системы, и применение в системе управления источника бесперебойного питания. В идеальном случае бесперебойное питание должно распространяться и на исполнительные органы, но это не всегда возможно. Обычно ограничиваются подключением только управляющего контроллера;

2. Возможность "горячей" замены модуля, как метода сокращения времени восстановления. Любой модуль в контроллере может быть изъят из коммутационной панели и установлен без отключения питания;

3. Резервирование контроллеров с "безударным" переключением при выходе из строя одного из контроллеров с использованием облегченного резерва, где резервирующие элементы находятся в менее нагруженном состоянии, чем основной резервируемый элемент. Вероятность бесперебойной работы такой системы определяется следующим образом:

$$P_C(t) = P_1(t) + \int_0^t P_2(t-\tau) f_1(\tau) d\tau,$$

где $P_1(t)$ – вероятность работы основного элемента в течение времени t, $P_2(t-\tau)$ – вероятность работы резервного элемента в течение времени t после переключения в момент времени τ.

$f_1(t) = -dP_1(t)/dt$ – функция изменения вероятности работы основного элемента по изменению времени t;

4. Перекрестная диагностика контроллерами состояния. Данная особенность позволяет повысить вероятность правильного принятия решения о переходе на резервную систему управления в случае возникновения отказа;

5. Резервирование линий передачи данных в систему верхнего уровня;

6. Резервирование линий передачи данных между контроллерами. Данный фактор влияет на отказоустойчивость системы в случае построения распределенной системы управления;

7. Резервирование линий обмена данными с контроллерами расширения ввода/вывода;

8. Наличие систем диагностики: работы всех составных систем контроллера, аппаратного отказа любого модуля в системе, диагностики измерительных трактов аппаратных модулей.

Выбор из вышеперечисленного списка факторов позволяет строить систему определенной стоимости и надежности [6].

ПЛК ЭЛСИ-ТМ с системой исполнения ЭлсиТМА предназначен для построения отказоустойчивых систем автоматизации. Архитектура контроллера предоставляет большой выбор способов резервирования элементов системы. Особенностью является то, что существует возможность произвольной комбинации способов резервирования в зависимости от специфики и бюджета проекта, а также требований к отказоустойчивости. Далее приведены основные способы резервирования отдельных элементов.

Резервирование электропитания

Резервирование электропитания обеспечивает непрерывную работу контроллера при отказе линии питания, первичного источника питания или других компонент системы электропитания. Существует множество вариантов подключения электропитания. Для примера на рис. 1 приводятся два способа подключения: от одной сети электропитания (вариант *А*) и от разных сетей электропитания (вариант *Б*).

Вариант *А* предполагает наличие двух независимых линий электропитания. Очевидно, что вариант *А* обеспечивает большую надежность, его применение особенно целесообразно, когда существует большая вероятность отказа одной из линий питания. По сравнению с вариантом *Б* схема подключения варианта *А* является более дорогой, так как подразумевает прокладку двух линий электропитания. В обоих вариантах предусмотрено резервирование источника питания (ИП), установленного в коммутационной панели контроллера.

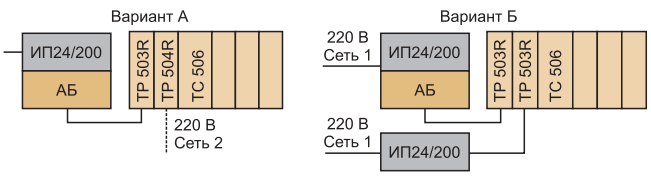

Рис. 1. Резервирование электропитания

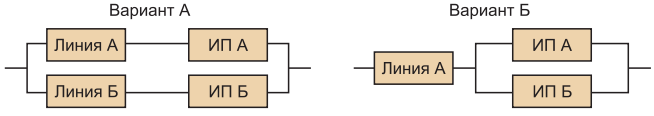

Рис. 2. Структурные схемы надежности вариантов резервирования электропитания

Рассмотрим структурные схемы надежности систем вариантов *А* и *Б* (рис. 2).

Рассмотрим следующие события: *А*1 – отказ первой линии электропитания; *А*2 – отказ второй линии электропитания; *Б*1 – отказ первого ИП; *Б*2 – отказ второго ИП.

Обозначим вероятность отказа первого ИП с первой линией

$$Q_A(C1) = Q(A1)+Q(B1).$$

Аналогично для второй линии и второго ИП:

$$Q_A(C2) = Q(A2)+Q(B2).$$

Вероятность отказа в таком случае для варианта *А* выглядит следующим образом:

$$Q_A = Q_A(C1)\cdot Q_A(C2|C1) = Q_A(C1)\cdot Q_A(C2)= \\ =Q(A1)\cdot Q(A2)+ Q(A1)\cdot Q(B2)+ \\ +Q(B1)\cdot Q(A2) + Q(B1)\cdot Q(B2).$$

Предположим, что вероятность линии питания и ИП одинакова, тогда вероятность отказа:

$$Q_A = 4\cdot Q(A1)\cdot Q(B1).$$

Как видно из предыдущего выражения минимальная степень вероятности отказа системы – вторая (с увеличением порядка уменьшается вероятность того или иного события).

Вероятность отказа варианта *Б*:

$$Q_Б = Q(A1)+ Q(B1)\cdot Q(B2).$$

Минимальная степень вероятности отказа системы – первая.

Резервирование контроллера

Резервирование базового контроллера обеспечивает непрерывную работу контроллера при выходе из строя различных элементов системы. Этот способ предполагает использование двух контроллеров (рис. 3), "мастер-модули" ТС506, которые соединены двумя разнотипными линиями связи. Один из контроллеров является основным – выполняет технологические задачи [7], другой – резервным. Резервный контроллер переходит в основной режим при отсутствии связи с основным контроллером по обеим линиям в течение заданного промежутка времени – основной признак сбоя.

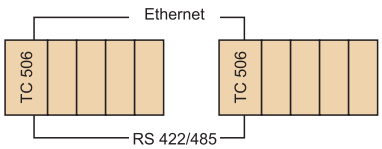

Рис. 3. Резервирование контроллера

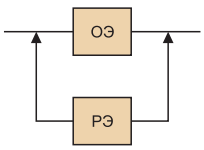

Рис. 4. Структурная схема надежности резервирования контроллера

Оба контроллера обмениваются информацией о своем состоянии. Это позволяет резервному контроллеру немедленно приступить к работе при обнаружении неисправности основного – выполнить функцию "горячего резервирования".

Основная особенность работы контроллера в том, что контроллер имеет возможность принудительного перехода в резерв по заданному пользователем алгоритму. В программе пользователя доступна информация о состоянии как основного, так и резервного контроллера в виде переменных задачи пользователя. Решение о переключении в резерв может быть принято, исходя из специфики конкретного проекта. Например, на основном контроллере вышел из строя модуль сигнализации о вскрытии щита, а на резервном отсутствует связь с объектом управления – выбор пользовательской программы "не переключаться" очевиден.

В дополнение для каждого контроллера может быть применена схема резервирования электропитания. Информация о состоянии линии питания также доступна программе пользователя.

Рассмотрим структурные схемы надежности системы с использованием облегченного резерва (рис. 4).

События системы: A – безотказная работа всей системы за наработку $(0, t)$; $A1$ – безотказная работа основного элемента (ОЭ) за наработку $(0, t)$, $P(A1) = P1(t)$; $A2$ – отказ ОЭ в момент времени τ, включение в работу резервного элемента (РЭ) и безотказная работа РЭ на интервале $(t - \tau)$, $P(A2) = P2(t)$.

Вероятность события А определяется как:

$$P(A) = P(A1) + P(A2). \quad (1)$$

Событие $A2$ является сложным и определяется как:

$$A2 = A21 \wedge A22,$$

где $A21$ – отказ ОЭ; $A22$ – безотказная работа РЭ.
Вероятность события $A2$ определяется по формуле:

$$P(A2) = P(A21) \cdot P(A22|A21).$$

Для определения $P(A21)$ рассмотрим малый интервал $(\tau, \tau + d\tau)$, для которого вероятность отказа ОЭ равна:

$$f_1(\tau)d\tau. \quad (2)$$

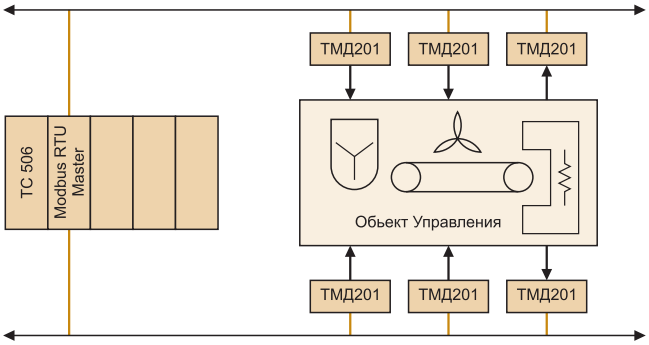

Рис. 5. Резервирование связи с объектом

Для получения вероятности отказа ОЭ проинтегрируем (2) по времени τ:

$$Q(t) = \int_0^t f(t)dt \text{ , тогда}$$

$$P(A21) = \int_0^t f(\tau)d\tau,$$

$$f_1(t) = -dP_1(t)/dt,$$

где $P1(\tau)$-вероятность бесперебойной работы ОЭ к моменту времени τ; $f(\tau)$ – плотность распределения отказов ОЭ к наработке τ.

Отсюда вероятность события $A2$ – отказ основного элемента, включение в работу резервного:

$$P(A2) = \int_0^t P_2(t-\tau) \cdot f_1(\tau)d\tau. \quad (3)$$

Определим при помощи выражений (1) и (3) вероятность безотказной работы системы с использованием облегченного резерва:

$$P_{C.OP}(t) = P_1(t) + \int_0^t P_2(t-\tau) \cdot f_1(\tau)d\tau. \quad (4)$$

Сравним полученный результат (4) с вероятностью безотказной работы системы с полным резервом:

$$P_{C.ПР}(t) = P_1(t) + \int_0^t P_2(t) \cdot f_1(\tau)d\tau \quad (5)$$

и с вероятностью безотказной работы системы без резерва:

$$P_{C.БР}(t) = P1(t). \quad (6)$$

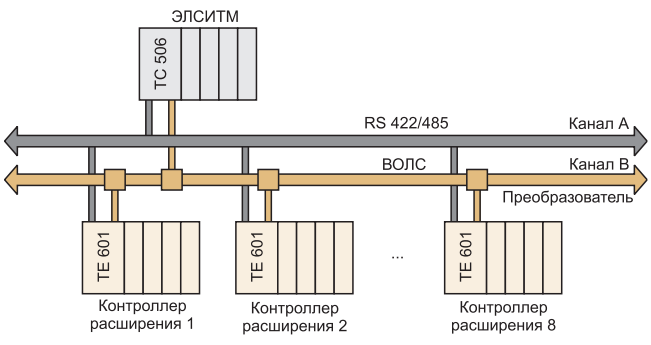

Рис. 6. Резервирование связи с контроллерами расширения

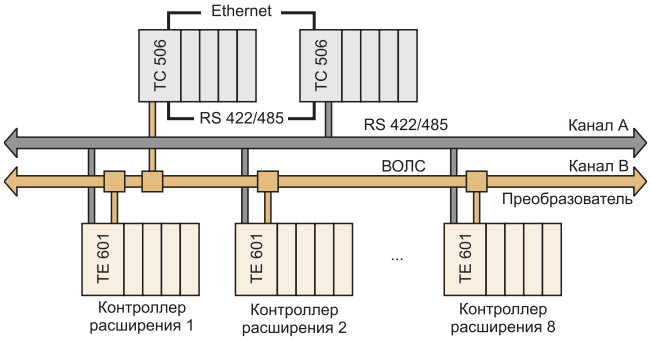

Рис. 7. Резервирование связи с КР и резервирование базового контроллера

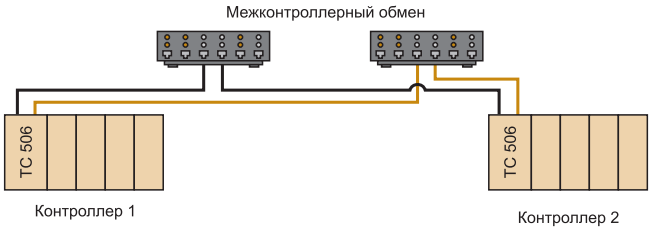

Рис. 8. Резервирование связи межконтроллерного обмена

Можно сделать вывод, что вероятность безотказной работы системы с полным резервом (5) меньше, так как наработка на отказ, а следовательно и вероятность отказа резервного контроллера в такой системе больше.

В системе без резервирования (6) вероятность безотказной работы (по сравнению с системами с облегченным резервом (4) и полным резервом (5)) наименьшая.

Резервирование связи с объектом управления

Связь с объектом управления осуществляется по протоколу Modbus RTU [8]. Для резервирования линий связи применяется двухканальный модуль (рис. 5). Резервирование связи с объектом управления может применяться совместно с резервированием системы электропитания (рис.1) и резервированием контроллеров (рис. 3).

Резервирование связи с контроллерами расширения

Контроллером расширения (КР) является контроллер, использующий в качестве "мастер-модуля" коммуникационный модуль ТЕ 601 и осуществляющий связь с "мастер-модулем" базового контроллера по фирменному протоколу с использованием канала

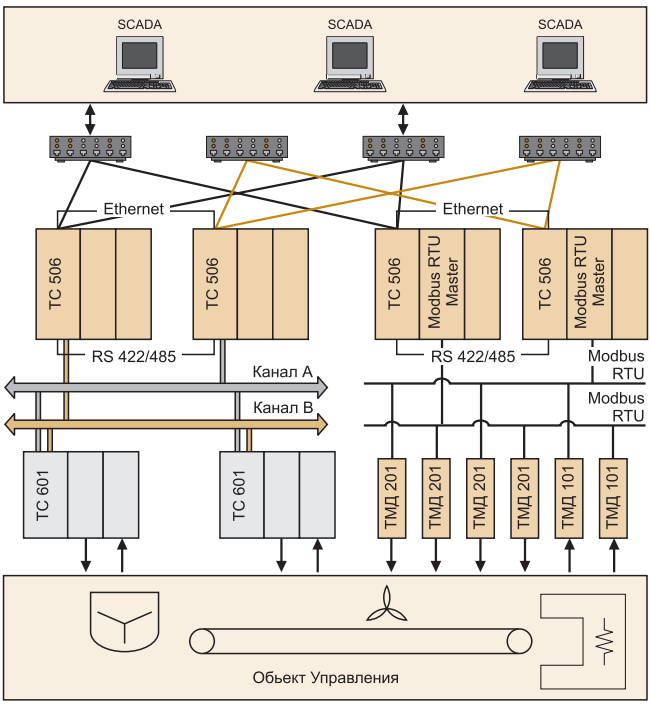

Рис. 10. Пример системы управления с резервированием

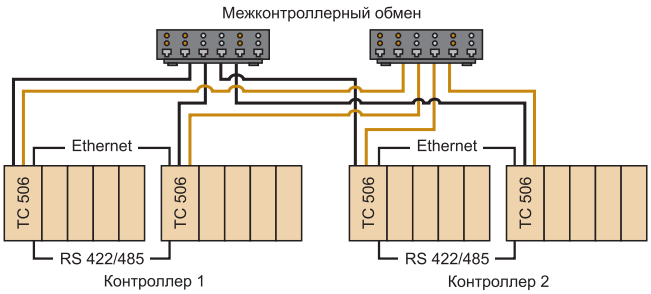

Рис. 9. Резервирование связи межконтролерного обмена с резервированием базового контроллера

RS-485/422 и/или волоконно-оптических линий связи (ВОЛС). На рис. 6 приведена схема резервирования связи с контроллерами расширения без резервирования базового контроллера.

Кроме того, резервирование связи с КР можно выполнить совместно с резервированием базового контроллера, при этом немного меняется схема подключения интерфейсов связи (рис. 7).

Резервирование канала связи межконтроллерного обмена

Как правило, в современных системах автоматизации существует обмен информацией между равноправными узлами – контроллерами. В таких случаях система становится критичной к отказам линий связи, по которым осуществляется обмен данными. В нашем случае предусмотрен вариант резервирования каналов связи межконтроллерного обмена. Обмен данными производится по фирменному протоколу, переход с одной линии связи на другую происходит автоматически при обнаружении неисправности. Понятие "узел" может означать как отдельный контроллер, так и контроллер с резервированием (рис. 3). Варианты подключения линий связи для обеспечения межконтроллерного обмена проиллюстрированы без резервирования базового контроллера (рис. 8) и с резервированием базового контроллера (рис. 9).

Резервирование связи с верхним уровнем (SCADA-системой) осуществляется по тем же принципам, что и при межконтроллерном обмене.

Для обобщения вышеприведенных вариантов построения системы управления технологическими объектами на рис. 10 представлен пример построения системы управления с резервированием каналов связи с верхним уровнем, резервированием связи

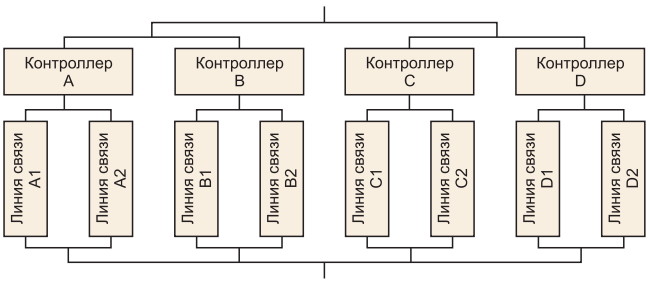

Рис. 11. Структурная схема надежности системы с полным резервированием объекта

межконтроллерного обмена, резервированием связи с контроллерами расширения и резервированием связи с модулями ввода/вывода.

Структурная схема надежности такой системы выглядит следующим образом (рис. 11). Обозначим событие отказа в соответствии с именем элемента, и тогда вероятность отказа данной системы будет выглядеть следующим образом.

Рис. 12. Структурная схема надежности без резервирования объекта

$$Q_C = (Q(A) + Q(A1) \cdot Q(A2)) \cdot (Q(B) + Q(B1) \cdot Q(B2)) \cdot (Q(C) + Q(C1) \cdot Q(C2)) \cdot (Q(D) + Q(D1) \cdot Q(D2)). \quad (7)$$

Предположим, что соответствующие элементы (контроллеры и линии) имеют одинаковую вероятность отказа, тогда выражение (7) преобразуется к виду:

$$Q_C = [Q(A) + Q(A1) \cdot Q(A2)]^4. \quad (8)$$

Минимальная степень вероятности отказа – четвертая. Сравним с системой без использования резервирования (рис. 12). Вероятность отказа такой системы будет определяться по следующей формуле:

$$Q_C = Q(A) + Q(A1). \quad (9)$$

Минимальная степень вероятности отказа – первая.

Таким образом, продемонстрированы варианты построения отказоустойчивых [9] систем автоматизации на базе контроллеров ЭЛСИ-ТМ. Одним из главных преимуществ является модульный подход к резервированию, позволяющий строить систему под индивидуальные потребности заказчика. Такая система обладает большой экономической и инженерной эффективностью.

Список литературы

1. *Кузьмин Ю.Б.* Типовой проект автоматизации технологических процессов на базе технологии Industrial Ethernet// Промышленные АСУ и контроллеры. 2005. № 1.
2. *Регентов А.В., Нестеренко П.Г.* Применение технологии коммуникационного контроллера в системах передачи технологической информации со сложной топологией. Контроллер ЭЛСИ-КОМ// Там же. 2006. № 3.
3. Надежность в технике. Основные понятия. Термины и определения. ГОСТ 27.002-89.
4. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. ГОСТ 34.003-90.
5. *Федоров Ю.Н.* Основы построения АСУТП взрывоопасных производств. В 2-х томах. Том 1 Методология. Москва: Синтег. 2006.
6. *Федоров Ю.Н.* Основы построения АСУТП взрывоопасных производств. В 2-х томах. Том 2 Проектирование. Москва: Синтег. 2006.
7. *Агафонов В.А.* OpenPCS – работаем с "железом! // itech – интеллектуальные технологии. 2006. февраль.
8. *Нестеренко П.Г., Климов А.В.* Связующее звено в технической системе// Там же. 2006. февраль.
9. Надежность и эффективность в технике / Под ред. А.И. Рембезы. Справочник в 10 т. Т. 1. Методология. Организация. Терминология. М.: Машиностроение. 1989.

Нестеренко Павел Геннадиевич *– заведующий отделом разработки ПО среднего уровня,*
Пачуев Константин Евгеньевич *– руководитель,*
Бухарин Иван Николаевич *– инженер-программист*
сектора разработки системного ПО отдела разработки ПО среднего уровня ЗАО "ЭлеСи".

Контактный телефон (382 2) 24-22-14.
E-mail: Pavel.Nesterenko@elesy.ru

Направления совершенствования структуры ПТК верхнего уровня управления АЭС

А.С. Тушков (НИИИС)

Предлагается вариант построения структуры ПТК системы верхнего блочного уровня (СВБУ), позволяющий реализовать как классическое дублирование элементов, так и функциональное резервирование.

В рамках работ по созданию АСУТП плавучей АЭС был проведен анализ существующих и возможных структур ПТК СВБУ с целью определения возможности совершенствования и использования их при построении ПТК СВБУ плавучей АЭС.

ПТК СВБУ служит для:

• централизации контроля и представления как обобщенной, так и детализированной информации о состоянии энергоблока, отдельных параметров ТП и состоянии оборудования;

• обеспечения дистанционного управления с рабочих станций (ПК) операторов-технологов оборудованием систем нормальной эксплуатации энергоблока и частью оборудования систем нормальной эксплуатации, важных для безопасности, управление которыми не предусмотрено с панелей систем безопасности (СБ);

• обеспечения возможности развития АСУТП путем внедрения дополнительных подсистем и перенастройки АСУТП;

• обеспечения необходимой информацией сменного персонала подразделений АЭС, которому эта информация необходима в процессе работы;

• обеспечения возможности обмена информацией со смежными ПТК и с общестанционным уровнем АСУТП.

ПТК СВБУ обеспечивает выполнение информационных, управляющих и вспомогательных функций СВБУ аналогично верхнему уровню управления любой другой АСУТП.